PRIMITIVES FOR FAST SECURE HASH FUNCTIONS AND STREAM CIPHERS

Techniques are disclosed to enable efficient implementation of secure hash functions and/or stream ciphers. More specifically, a family of graphs is described that has relatively large girth, large claw, and/or rapid mixing properties. The graphs are suitable for construction of cryptographic primitives such as collision resistant hash functions and stream ciphers, which allow efficient software implementation.